POR-FESR EMILIA ROMAGNA 2014-2020

Asse 1 - Ricerca e innovazione

Azione 1.2.2 - Supporto alla realizzazione di progetti complessi di attività di ricerca e sviluppo su poche aree tematiche di rilievo e all'applicazione di soluzioni tecnologiche funzionali alla realizzazione della strategia di S3

Bando 2018

Progetti di ricerca industriale strategica rivolti agli ambiti prioritari della Strategia di Specializzazione Intelligente

Sistemi interoperabili ed efficienti per la gestione sicura di filiere industriali

Deliverable D2.2:
Specifiche del sistema SmartChain

Data di consegna prevista:	31 Dicembre 2020
Autori:	CIRI ICT, CRIS, CROSSTEC, MECHLAV, TTLAB
Versione:	1

Indice

1. Modelli di blockchain adottati

Il progetto Smart Chain ha come scopo la realizzazione di una piattaforma basata su tecnologia blockchain per il supporto e la certificazione della filiera industriale. Il progetto prende in considerazione casi di studio diversificati, uno nell'ambito della filiera agroalimentare del parmigiano reggiano con il coinvolgimento del consorzio parmigiano reggiano, uno nell'ambito della filiera manifatturiera dell'azienda Carpigiani e infine, uno nell'ambito della filiera tessile con l'azienda Biancoaccessori. In particolar modo, il progetto si focalizza sulla progettazione e realizzazione di due scenari specifici, quello Carpigiani e Biancoaccessori.
In questa fase del progetto sono stati scelti il modello e l'implementazione di blockchain da utilizzare partendo dall'analisi dello stato dell'arte delle piattaforme blockchain e dei requisiti dei casi di studio condotta nella prima parte del progetto. La blockchain è il componente core dell'infrastruttura su cui si basano tutti i layer software superiori ed è fondamentale per mantenere inalterabili e con un preciso ordine cronologico i dati inseriti.

Per il progetto sono stati scelti modelli di blockchain differenti in base alle peculiarità e alle esigenze degli specifici casi d'uso e a diversi parametri di confronto delle blockchain (modello di governance, costi, modello di gestione). In particolare, l'esigenza dell'azienda Biancoaccessori è quella di sviluppare un meccanismo di notarizzazione per garantire i rapporti tra committente e cliente e il possesso delle certificazioni necessarie. I rapporti tra aziende diventano infatti fondamentali quando si tratta di ordini ingenti e c'è la necessità di sapere se dietro un ordine vi sia effettivamente una grossa azienda. Mentre l'esigenza dell'azienda Carpigiani è quella di servitizzazione ovvero l'esercente prende in leasing una macchina (nessun costo di acquisto upfront) e il costo di tale leasing è parametrato sull'effettiva produzione di gelato; nel canone di leasing è compresa anche la fornitura degli ingredienti da parte di un produttore selezionato da Carpigiani stessa. In questo caso si vuole certificare la produzione del gelato e il relativo consumo degli ingredienti, considerando che tra gli attori vige un rapporto di parziale fiducia reciproca.

1.1 Caso Biancoaccessori ed Ethereum

Nel caso d'uso Biancoaccessori si è optato per un modello permissionless utilizzando la blockchain Ethereum. Ethereum è un progetto open-source ampiamente diffuso e utilizzato e ha un ottimo supporto allo sviluppo degli smart contract. Il modello di blockchain pubblico consente di mantenere il deployment e la manutenzione del ledger (gestione server, aggiornamenti, etc) indipendente dalle aziende coinvolte nel progetto che quindi non devono accollarsi l'onere di gestire la piattaforma e offre una legittimazione forte grazie alla partecipazione di un alto

numero di nodi. Lo svantaggio di questo modello è però il pagamento per ciascuna transazione di una fee per l'utilizzo della piattaforma.

Una volta stabilito il tipo di blockchain ci si è focalizzati sullo smart contract che è il protocollo che si occupa dell'esecuzione di un contratto e dell'interazione con i relativi dati da parte delle varie aziende. Abbiamo così definito la struttura a livello di interfacce di comunicazione e di interoperabilità e il linguaggio di programmazione da utilizzare. Sono stati inoltre analizzati aspetti di sicurezza come la visibilità dei metodi degli smart contract e la conservazione e protezione dei dati sensibili inseriti.

La scelta del linguaggio di programmazione è ricaduta su Solidity cha ha un buon supporto, un'architettura consolidata e un'ampia community. Per quanto riguarda invece la visibilità dei metodi, essa viene gestita attraverso alcune parole chiave come ad esempio "private" che rende non ereditabile il metodo e ai modifiers che restringono l'utilizzo della funzione ai solo utenti specificati.

Poichè si è optato per una blockchain pubblica tutto ciò che si utilizza in un smart contract è pubblicamente visibile, comprese le variabili locali e le variabili di stato contrassegnate come private, i contratti sono infatti sono visualizzabili da tutti in bytecode su ciascun peer della blockchain. Questo caratteristica ha influenzato fortemente la progettazione dell'architettura perché i dati sulla blockchain hanno la necessità di essere mantenuti riservati. E' stato così necessario introdurre uno strato intermedio per ricevere le chiamate dal client, criptare i dati da inserire nella blockchain e gestire le relative chiavi di cifratura.

1.2 Caso Carpigiani e Hyperledger Fabric

Nel caso d'uso Carpigiani ci si è invece orientati per una blockchain di tipo permissioned utilizzando come implementazione il progetto open-source Hyperledger Fabric. La scelta di una blockchain privata è giustificata dal fatto che i dati relativi alle quantità di ingredienti utilizzati da ciascun esercente sono da considerarsi delle informazioni commercialmente rilevanti di cui garantire la privacy. Infatti, produttori di ingredienti diversi che riforniscono lo stesso esercente devono poter accedere ai soli dati relativi ai loro prodotti e non a quelli di altri produttori concorrenti. Inoltre, in questo caso, per l'azienda non risulta essere un problema la gestione e manutenzione della piattaforma blockchain privata.

Si è scelto di adottare Hyperledger Fabric in quanto è risultato essere la soluzione più adatta per i seguenti aspetti:

- affidabilità delle aziende coinvolte: il progetto Hyperledger vede la collaborazione di più di 200 aziende ed altre illustri realtà come la Linux Foundation, IBM, Intel, Fujitsu, e molte altre;

- architettura di base: Hyperledger Fabric risulta essere molto versatile, grazie alla sua struttura modulare, che rende semplice la modifica o l'introduzione all'interno della Blockchain di una nuova organizzazione e/o di nuovi nodi;
- Smart Contract realizzati attraverso una vera e propria istanza di un programma che viene installato e mantenuto da tutti i nodi in grado di interagire con il registro della Blockchain, realizzabili attraverso differenti linguaggi di programmazione (Go, Java e Node.js) e altamente personalizzabili.
- prestazioni: Hyperledger Fabric è in grado di garantire ottime prestazioni grazie ad un sapiente utilizzo dei canali (partizioni virtuali della rete) e grazie alla suddivisione del lavoro tra più entità (endorser, committer, orderer e client).

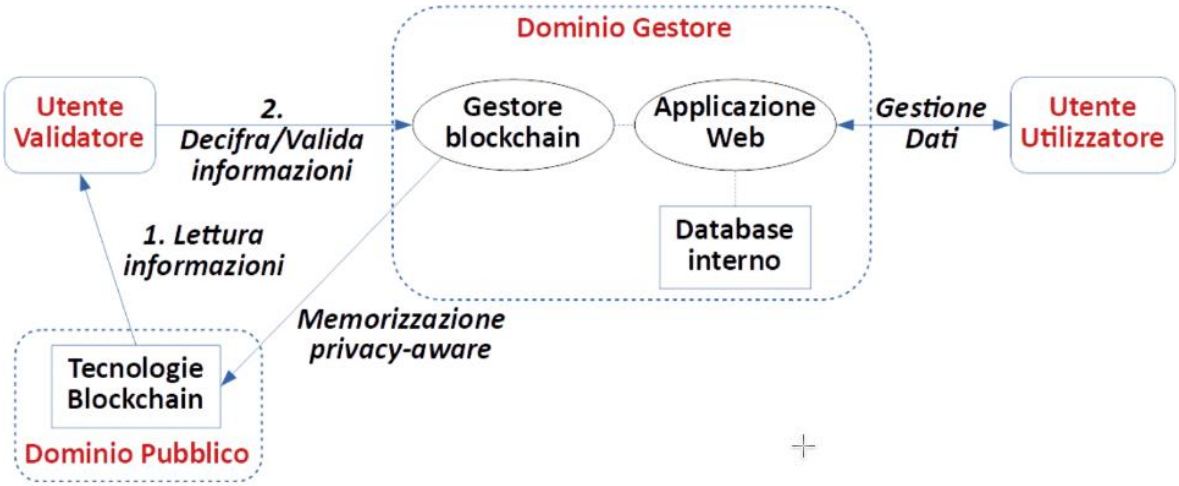
Si noti inoltre che Hyperledger sta sempre più diventando la piattaforma di riferimento per quanto riguarda il mondo della Blockchain in ambito business.

2. Modellazione dei sistemi

2.1 Modellazione Biancoaccessori

Il sistema è incentrato sulla creazione di una rete di imprese che permetta di dimostrare l'impiego di pratiche virtuose e dell'impiego di fornitori altrettanto virtuosi. Il sistema è pensato per funzionare anche in un ambito parzialmente digitalizzato,in cui parte le imprese registrate si rivolgono a fornitori non presenti nel sistema, ma che possono comunque essere in grado di fornire certificazioni di qualità attestanti, ad esempio, la propria organizzazione o le modalità di gestione dei propri processi produttivi. Tecnicamente, il sistema mira alla definizione di un profilo per ogni impresa, che definisce i suoi fornitori. Ogni impresa è dotata di certificazioni che ne attestano diverse caratteristiche (ad esempio, conformità a standard o soddisfazione di requisiti in ambiti organizzativi o di processi). Ogni impresa fornisce documentazione attestante le certificazioni digitali. Ogni fornitore di un'impresa potrebbe essere anch'essa un'impresa registrata nel sistema, oppure un'impresa non registrata. Nel primo caso, il sistema collega direttamente le certificazioni dichiarate di ciascuna impresa per estrarre le informazioni necessarie. Nel secondo caso, l'impresa si prende carico di fornire le informazioni di certificazione per conto dei propri fornitori senza poter caricare la documentazione originale. Il sistema ha cura di gestire in modo opportuno i requisiti di privacy delle imprese nell'ambito delle certificazioni, delle documentazioni e della rete dei fornitori. L'obiettivo è di creare un sistema di tracciatura che consente un accesso multilivello alle informazioni mantenute, consentendo ad esempio l'accesso ad informazioni aggregate e non identificative a un alto numero di soggetti, mentre altre informazioni potrebbero essere accedute soltanto a un ristretto gruppo di entità o ad entità selezionate. Ad esempio, alcune informazioni potrebbero essere pubbliche e disponibili a tutti, altre solo alle imprese facenti parte del sistema, altre ancora solo a destinatari selezionati

Per ottenere l'opportuno trade-off in termini di tracciabilità, funzionalità e privacy, il sistema proposto si basa sull'integrazione di soluzioni di mantenimento delle informazioni basate su paradigmi blockchain e su sistemi di gestione dei dati tradizionale. In questa fase ci siamo preoccupati di capire di quali informazioni e funzionalità si occupano ciascuno di questi due macro-componenti, identificando inoltre le modalità di comunicazione fra di essi, incluse le interfacce di collegamento e i componenti comuni. Ciascun macro-componente è stato dettagliato nel paragrafo successivo mentre il sistema è concettualmente rappresentato nella figura sottostante.



Il sistema viene realizzato tramite un'architettura decentralizzata in quattro classi di dominio principali:

- dominio pubblico - si considera di utilizzare la tecnologia blockchain permissionless Ethereum
- dominio gestore - per ottenere il dovuto trade-off fra funzionalità, sicurezza e usabilità, si è introdotta un componente intermedio che si preoccupa di gestire un'applicazione Web, un database interno con tutte le informazioni, e gestisce l'interazione con la blockchain tramite un componente qui chiamato gestore blockchain;
- La piattaforma viene acceduta da diversi utenti, si evidenziano due tipi di utenti principali:
    - gli utenti utilizzatori che accedono alla piattaforma tramite un sito Web per gestire in modo completo le informazioni (ad esempio, le imprese che vogliono avvalersi della piattaforma o altri tipi di utenti che devono accedere alle informazioni complete delle imprese). Questi utenti si fidano del gestore come intermediario per la gestione dei dati su blockchain;
    - gli utenti validatori (ad esempio, enti per il controllo dei dati e delle certificazioni) che accedono ai sistemi blockchain tramite software eseguito da loro stessi, e possono verificare che le informazioni memorizzate sulle tecnologie blockchain sono legittime. In alcuni casi, ad esempio per accedere a informazioni confidenziali, gli utenti devono interagire con il gestore blockchain della piattaforma, ma da un punto di vista del modello di fiducia e dei protocolli

impiegati non viene richiesto che i validatori assumano che questo componente sia fidato

2.1.1 Descrizione dettagliata delle informazioni

Le informazioni gestite all'interno del sistema consistono invece in:

- **Impresa registrata**: dati strutturati che descrivono le caratteristiche di un'impresa registrata nel sistema
- **Fornitore (impresa registrata o non registrata)**: è tipicamente un'impresa registrata che ha un contratto di fornitura con un'altra impresa
- **Certificazione**: dati strutturati che attestano diverse caratteristiche di conformità;
- **Documentazione**: dato non strutturato che rappresenta la digitalizzazione di un documento ufficiale "cartaceo" che rappresenta e dimostra delle certificazioni dell'azienda.

Queste informazioni possono essere gestite in maniera largamente differente all'interno del sistema, consentendo, ad esempio, la completa tracciabilità e visibilità pubblica per alcune di esse, gestendo invece altre attraverso sistemi ad accesso privato. La discussione sulla gestione dei sistema di protezione dei dati è rimandata alle fasi di progettazione seguenti, sia perché, come appena descritto, le informazioni potrebbe essere gestite in modo largamente differente e avere requisiti di protezione differenti, sia perché la rilevanza di alcune informazioni può essere misurata solo quando contestualizzata rispetto alle funzionalità in cui sono utilizzate (ad esempio, potrebbe essere necessario proteggere le informazioni di relazioni nella rete di imprese, che al momento non sono ancora modellate e considerate).

Ecco più nel dettaglio la lista completa delle informazioni dei dati strutturati che si ritiene essere necessario gestire nel sistema progettato:

<u>Impresa</u>

- identità legale: identificatore legale dell'impresa; es. partita IVA
- Ragione Sociale
- PEC
- Nome della persona che ha chiesto la registrazione(esempio: titolare dell'impresa)
- Documentazione identità: documentazione associata all'impresa (es. pdf della carta di identità)
- Sede legale (esempio: indirizzo)
- Certificazioni: lista delle certificazioni in possesso dell'impresa
- Documenti di certificazione
- Lista dei rapporti di fornitura

- Altre informazioni di profilo critiche relative agli anni (esempio: fatturato, numero di ordini, volume merci in ingresso/uscita,volume produzione annuo, numero dei dipendenti, ammontare dei pagamenti ai dipendenti, ecc.)

Fornitore (impresa non registrata)

- identità legale: identificatore legale dell'impresa (es. P. IVA)
- nome impresa
- Ruolo
- distretto: inquadra il luogo in modo lasco
- data inserimento dell'informazione (ha durata un anno)
- certificazioni: lista delle certificazioni in possesso dal fornitore

Certificazione

- descrizione: descrizione informale del contenuto della certificazione
- issuer: identificatore di chi rilascia il certificato
- type: tipo della certificazione
- object: oggetto della certificazione (organizzazione, processo, prodotto),eventualmente con diciture gerarchiche
- subject: impresa certificata
- validità: periodo temporale di validità della certificazione

2.1.2 Funzionalità principali di Biancoaccessori

Progettiamo un sistema prototipale in cui ci focalizziamo sul fornire le seguenti funzionalità:

1. **Mostrare informazioni/certificati dell'impresa**
2. **Lista dei fornitori di un'impresa** (senza mostrare partite IVA o informazioni identificative). Ad esempio, senza mostrare l'indirizzo preciso, ma mostrando informazioni di luogo (esempio: provincia) e il ruolo (esempio: cosa fornisce -tintura, tacchi, ... -)
3. **Accedere al dettaglio sulle certificazioni del fornitore**, ovvero ad esempio oltre al luogo, e al ruolo, fornire la lista delle certificazioni di un fornitore, sempre senza dare informazioni di identificazione;
4. **Sapere quali fornitori rispettano certe caratteristiche**. Ad esempio, quanti fornitori hanno il DURC. Queste funzionalità sono di "default" accedute utilizzando le informazioni più aggiornate.

Ipotizziamo inoltre che non ci interessi impedire anche un accesso "storico" alle informazioni passate e che potrebbe essere utile dare la possibilità di modificare i dati inseriti, ipotizzando che sia possibile che qualcuno faccia un errore nell'inserimento. Inoltre, una funzionalità potenzialmente interessante è anche quella di permettere l'accesso ai dati identificativi dei fornitori a un committente.

Il sistema deve essere in grado di gestire delle autorizzazioni per capire quali utenti possono effettuare queste operazioni. Idealmente, le scelte che guidano se concedere le autorizzazioni si basano su molteplici fattori:

- sulla base del ruolo, come nel caso di Admin, Imprese o Utenti validatori
- sulla base delle proprietà di accesso associate a ciascuna specifica risorsa, nell'ambito dei "proprietari" di ciascuna risorsa (ogni impresa è "proprietaria" e responsabile dei dati dell'impresa caricati, come ad esempio in un file system) e di utenti che possono stati delegati ad accedere a quei dati dall'impresa proprietaria (stile Access Control List)

Nella seguente tabella si cerca di enumerate le operazioni di autorizzazione necessarie.

Operazione	Autorizzazione (azione/risorsa)	Policy	Note
Registrazione nuova impresa	Crea/Impresa	Solo 'admin' può farlo	Admin idealmente sarebbe un ruolo nell'applicazione
Inserimento fornitore esterno	Crea/Fornitore	Impresa può aggiungere solo forniture riguardo sé stessa	
Inserimento fornitura impresa interna	Crea/Fornitura	Impresa può aggiungere solo forniture riguardo sé stessa	Sarebbe ipotizzabile inserire un sistema di "doppia" validazione, in cui anche l'impresa indicata come fornitrice acconsente a essere tale
Creazione certificazione propria	Crea/Certificazione	Impresa può creare una certificazione solo per sé stessa	
Creazione certificazione fornitore esterno	Crea/Certificazione	Impresa può creare una certificazione solo per fornitori esterni a lei associati	
Accesso a dati risorsa	Leggere/<risorsa>	L'entità è stata delegata dall'impresa proprietaria a leggere i dati	Per <risorsa> si intende una qualsiasi risorsa, che può essere un'impresa, una fornitura, una certificazione o una documentazione, ad esempio. Questo

			approccio inizialmente può essere “flat”, ovvero l’accesso a ciascuna risorsa è indipendente da permessi di accesso ad altre risorse. In versioni successive è però probabile chesi vorrà creare un sistema di accesso gerarchico per rendere più efficiente l’accesso, ad esempio, a “tutte” le certificazioni di una certa impresa.

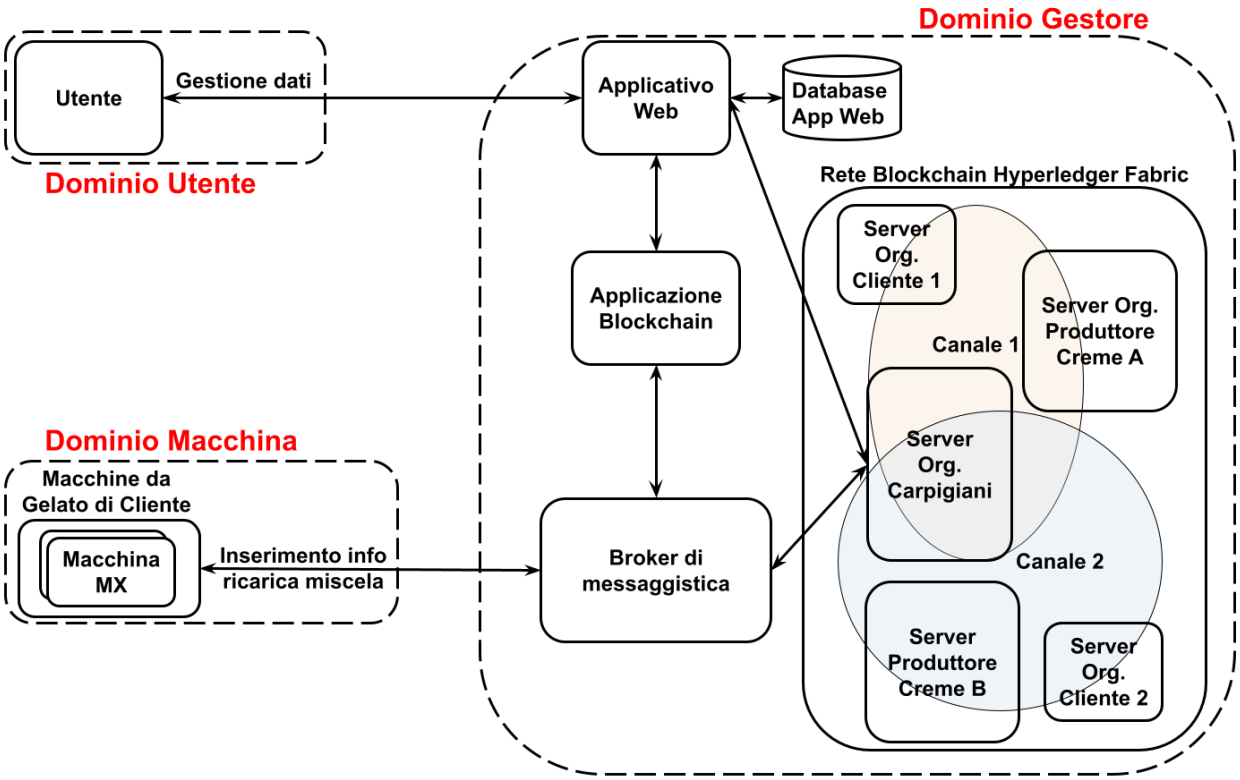
2.2 Modellazione Carpigiani

Le tipologie di attori partecipanti alla rete Blockchain individuati, sono:

- Carpigiani: l'azienda di riferimento abilitata a partecipare a tutte le transazioni che avvengono nella rete;
- fornitori/produttori di miscele: tutte le aziende con le quali Carpigiani ha stretto accordi e sono abilitati a partecipare alla rete;
- utilizzatori delle macchine/esercenti: coloro i quali hanno accordi sia con Carpigiani che con uno o più fornitori dai quali dovranno rifornirsi.

Dato che Carpigiani ha la necessità di mantenere riservati i dati inerenti alle transazioni per instaurare una forma di fiducia anche tra concorrenti che partecipano alla rete, è stata considerata un'architettura basata su canali in cui risiedono solamente tre attori: Carpigiani, un’azienda fornitrice di miscela per il gelato e un esercente/utilizzatore finale della macchina.
I canali, per definizione, permettono di creare una Blockchain privata dove sono garantiti l'isolamento e la confidenzialità delle informazioni scambiate tra organizzazioni (attori) differenti e possibilmente concorrenti senza, però, ledere la privacy. Pertanto viene creato un canale per ogni terna di attori, dove in ogni canale è presente Carpigiani, mentre gli altri due attori corrispondono sempre ad un fornitore e all’esercente. In questo modo è possibile consentire accordi commerciali diversi a seconda del fornitore o dell’esercente coinvolto.

Inoltre, far partecipare un numero limitato di entità all'interno di un canale consente di realizzare una struttura facile da gestire e allo stesso tempo molto sicura (alta diffusione del ledger condiviso tra tutti gli attori), risultando vantaggiosa grazie al limitato traffico generato da una rete peer-to-peer con pochi nodi che devono partecipare al consenso di un canale e non di tutta la rete permettendo anche una dimensione contenuta del ledger.
Il sistema è rappresentato nella figura sottostante.



Il sistema viene realizzato seguendo tre classi di dominio:

- il **dominio utente** che ha il compito di gestire le informazioni registrate nella blockchain accedendo ad un applicativo Web;
- il **dominio gestore** che comprende:
    - la rete Blockchain suddivisa in canali e contenente le tre tipologie di attori descritti in precedenza;
    - un'applicazione Blockchain per la configurazione e modifica della rete Blockchain;
    - un broker di messaggistica per disaccoppiare e gestire concorrentemente l'inserimento dei dati di refill e la gestione dei canali della rete Blockchain
    - un applicativo Web per la presentazione all'utente delle informazioni contenute nella blockchain e per consentire al gestore di apportare le principali modifiche alla Rete Blockchain in modo semplificato;

- il **dominio macchina** che ha il compito di inserire nella blockchain le informazioni relative alla ricarica della miscela (refill) attraverso un software in esecuzione sulle macchine da gelato.

2.2.1 Descrizione dettagliata delle informazioni

Le informazioni gestite all'interno del sistema consistono in:

- **Utente**: dati strutturati che identificano e informazioni relative ad una persona appartenente ad un'azienda coinvolta
- **Organizzazione**: dati strutturati che identificano in modo univoco le aziende coinvolte
- **Canale**: dati strutturati che identificano in modo univoco il canale della Blockchain che racchiude la terna (Carpigiani/fornitore di miscele/esercente)
- **Smart Contract**: dati non strutturati costituiti dal codice sorgente relativo alle funzioni utilizzabili in uno specifico canale
- **Macchine**: dati strutturati che identificano in modo univoco un oggetto macchina da gelato
- **Refill**: dati strutturati indicanti l'operazione di ricarica della miscela in una macchina da gelato.

<u>Utente</u>
- Email: identificativo dell'utente
- Admin: tipologia dell'utente collegato se admin (Carpigiani) o utente normale (rappresentante dell'azienda produttrice dei refill o esercente)

<u>Organizzazione</u>
- Nome: il nome dell'azienda
- Partita iva
- Sede centrale dell'azienda

<u>Canale</u>
- Nome: Identificativo univoco del canale

<u>Macchine</u>
- Nome: Identificativo della macchina
- Organizzazione: azienda che la possiede in pay-per-use

<u>Refill</u>
- Macchina: il nome identificativo della macchina in cui è stato effettuato il refill
- Barcode: codice a barre del prodotto versato in fase di refill inerente all'azienda produttrice
- Produttore: identificativo dell'azienda produttrice della miscela usata in fase di refill

- Quantità: quantità in litri di prodotto versato in fase di refill
- Timestamp barcode: registrato momento esatto in cui è stato letto il codice a barre del prodotto
- Timestamp refill: momento esatto in cui è stato effettuato il refill
- Coni: indice di quanti coni sono stati erogati complessivamente fino al nuovo refill
- Contratto: codice e versione dell'accordo finanziario stabilito utile a mantenere aggiornata l'informazione.

2.2.2 Funzionalità principali di Carpigiani

Le principali funzionalità realizzate per il caso di Carpigiani riguardano:

- **Visualizzazione delle informazioni di refill** delle macchine da gelato
- **Gestione delle macchine da gelato**
- **Gestione della rete blockchain** (Canali, Organizzazioni, Smart Contract…)

Nello specifico si è pensato di ridurre al minimo l'onere di gestione dell'infrastruttura nei confronti del personale afferente agli esercenti e alle aziende fornitrici di miscela, in quanto con ogni probabilità non disporranno di personale tecnico con un background informatico particolarmente elevato.
L'accesso alle funzionalità presentate è consentito unicamente previo login di un utente alla piattaforma web che consente due tipologie di utenti, uno senza privilegi (di seguito denominato user) e uno con privilegi (denominato admin).
Per quanto riguarda gli utenti admin hanno accesso alle informazioni di tutte le macchine presenti nella blockchain, mentre gli utenti user possono consultare unicamente le macchine e i relativi refill afferenti alle macchine della propria organizzazione.
Nella seguente tabella sono enumerate le operazioni consentite della piattaforma web.

Operazione	**Autorizzazione (azione/risorsa)**	**Policy**	**Note**
Aggiunta di un utente	Crea/Utente	Solo admin può farlo	
Aggiunta di una macchina	Crea/Macchina	Solo admin può farlo	
Creazione di un nuovo canale	Crea/Canale	Solo admin può farlo	
Creare una nuova organizzazione	Crea/Organizzazione	Solo admin può farlo	
Creare un nuovo refill	Crea/Refill	Solo macchina può farlo	
Installazione nuovo	Crea/Smart Contract	Solo admin può farlo	Viene diffuso lo smart

smart contract su un canale			contract all’interno del canale rendendolo accessibile agli attori
Visualizzazione elenco macchine	Leggere/Macchine	Solo user registrato può farlo	Ogni utente può accedere unicamente all’elenco delle proprie macchine
Visualizzazione refill singola macchina	Leggere/Refill	Solo user registrato può farlo	Ogni utente può accedere unicamente ai refill appartenenti alle proprie macchine